Bank		**Date of Exam**	
Charter		**Prepared By**	

#17 - Account Takeover Risks

ASSIGNMENT OVERVIEW

Account Takeover is a type of identity theft where thieves gain control of existing financial accounts by obtaining personal information such as account number and social security number. The thieves use that information to take over existing bank and credit card accounts.

Corporate Account Takeover is a form of business identity theft where cyber thieves gain control of a business' bank account by stealing employee passwords and other valid credentials. Thieves can then initiate fraudulent wire and ACH transactions to accounts controlled by the thieves. Businesses with limited or no internal computer safeguards and disbursement controls for use with the bank's online banking system are vulnerable to theft when cyber thieves gain access to their computer systems, typically through malicious software (malware). Malware infects a business' computer system not just through 'infected' documents attached to an email but also simply when an infected Web site is visited.

A task force of bankers in Texas worked with the U.S. Secret Service to develop recommended practices to mitigate the risks of electronic crimes such as corporate account takeover. The Task Force developed a list of 19 recommended processes and controls which expand on a three-part risk management framework of: 1) Protect; 2) Detect; and 3) Respond. The Task Force also developed *Best Practices for Reducing the Risks of Corporate Account Takeovers* (*Best Practices*) to help banks establish specific practices to implement the recommended processes and controls. The *Best Practices* document is a valuable resource to effectively reduce risk. For more information on the practices offered by the Task Force, go to www.ectf.dob.texas.gov.

The FFIEC released *Supplement to Authentication in an Internet Banking Environment* (FFIEC Supplemental Guidance) on June 28, 2011, which reinforces previous FFIEC guidance related to risk management of online transactions and updates regulatory expectations regarding customer authentication, layered security, and other controls related to online activity. The Task Forces' recommended three-part Corporate Account Takeover risk management framework and related controls are similar to controls in the FFIEC Supplemental Guidance and include the practices recommended by the FFIEC guidance. The Task Force guidance differs from the FFIEC Supplemental Guidance in that it has a more specific focus on reducing the risk of Corporate Account Takeovers and therefore provides additional steps to implement.

The Department issued Supervisory Memorandum 1029 regarding Standards for the Risk Management of Corporate Account Takeovers which requires bank management and the board of directors to address each of the 19 components in a risk management program to mitigate the risk of Corporate Account Takeover. These components also apply to retail customer account takeover as well.

CORE PROCEDURE – ACCOUNT TAKEOVER RISK

Initial Risk Assessment

Assess the account takeover risk to determine if this procedure should be performed.

1a. Determine the probability of an Account Takeover (ATO) of a consumer or corporate account. If the risk is low or nonexistent, then an ATO program is not necessary at this financial institution at this time. The risk is high if the bank offers any of the following products through the electronic banking or cash management system for either commercial or retail customers:

- Wire transfer requests;
- ACH origination requests;
- External account transfers; and/or
- Person to Person Pay (P2P).

Examiner Comments:

1b. Determine whether deficiencies noted in the last examination and most recent internal/external audit have been addressed and/or corrected by management for an ATO program. Detail how deficiencies were corrected. *Include copy of audit exceptions and/or prior examination criticisms and management response in work papers, or summarize exceptions/criticisms below or indicate the page number in the last examination report where deficiencies are noted, if applicable.*

Examiner Comments:

PROTECT: Bank Awareness, Services Offered and Risk Profile

Assess awareness of account takeover risk, the types of electronic banking services offered, and the bank's risk profile. Tools and resources are available on the Texas Banker's Electronic Crimes Task Force webpage (www.ectf.dob.texas.gov) to assist the institution in implementing a strong ATO Protection program.

2a. Verify that the board has discussed the risks associated with Account Takeover. This should be documented in the board minutes.

Examiner Comments:

2b. Evaluate the methods implemented to enhance authentication or layered security, as detailed in the FFIEC guidance and (P6) of the CATO Best Practice guidance (Best Practices). Describe the methods and indicate if adequate. Describe any weaknesses.

Examiner Comments:

2c. Review and evaluate the adequacy of the institution's information security risk assessment which should include threats related to ATO. Refer to (P1) of the Best Practices. A sample risk assessment is available on the Texas Banker's Electronic Crimes Task Force webpage at www.ectf.dob.texas.gov. Indicate if adequate and describe any weaknesses.

Examiner Comments:

2d. Describe and determine if the institution's method for risk rating on-line banking customers is reasonable. Refer to (P2) of the Best Practices.

Examiner Comments:

2e. Describe and evaluate the bank's efforts to educate:

1) Corporate online banking customers on basic online security practices as suggested in (P4) of the Best Practices. (i.e. keeping anti-virus and system software up to date, using strong passwords and dual controls, transmitting ACH files and wire instructions securely, etc.). Refer to Appendix on Security Awareness Education for Customers;
2) Retail and high risk customers on additional security awareness as suggested in (P5) of the Best Practices; and
3) Corporate account holders on the detection of fraudulent account activity. Refer to (D3) of the Best Practices. This would include monitoring for a change in login credentials, loss of computer speed, unexpected rebooting, new toolbars, and inability to shut down computer.

Examiner Comments:

2f. Determine if signed written agreements are in place with corporate and retail customers using online banking services and if those agreements have been reviewed by legal counsel in light of ATO issues. Refer to (P7) of the Best Practices. *Note: Retail customers do not necessarily need written agreements but in some circumstances they may have them.*

Examiner Comments:

DETECT: Monitoring Systems, Employee Awareness, Notifications From Customers

Assess bank's ability to detect electronic theft through monitoring systems, employee awareness, and notifications from customers.

3a. Evaluate and comment on the bank's monitoring system, controls for system administrators, and processes to detect anomalies. Describe any weaknesses. Determine if management has evaluated all reasonable detection options based on the risk profile of the corporate online banking environment. Refer to (D1) of the Best Practices. Detection options may include a manual review for low transaction volumes, or an automated system that can detect red flags in a high volume environment.

Examiner Comments:

3b. How are bank personnel notified of a detected anomaly in an automated system? Refer to (D1.4) of the Best Practices. Determine if the bank's practice is adequate.

Examiner Comments:

3c. Does the bank employee education and training program appear adequate to detect fraudulent account activity? Refer to (D2) of the Best Practices. This would include educating employees to monitor for a change to a corporate customer's online banking profile; unusual customer activity; and, to recognize compromised internal systems at the bank.

Examiner Comments:

RESPOND: Incident Response and Notification

Assess the bank's incident response plans and procedures.

4a. Review and determine if the bank has adequate written policies and procedures and incident response plan for addressing account takeovers. Describe any weaknesses.

Examiner Comments:

4b. Do bank employees have multiple methods to contact a customer immediately in the event of suspected fraudulent activity? Refer to (R2) of the Best Practices. Describe the methods and determine if practices are acceptable.

Examiner Comments:

4c. Does the incident response plan include procedures to:

1) Attempt to immediately reverse fraudulent transactions? Refer to (R3) of the Best Practices. Do procedures include FedLine's "Fraudulent File Alert" and/or notification to receiving bank? ;
2) Suspend any compromised systems? Refer to (R6) of the Best Practices;
3) Contact law enforcement and regulatory agencies once the initial recovery efforts have concluded? Refer to (R7) of the Best Practices; and
4) Handle customer relations and documentation of recovery efforts? Refer to (R8) of Best Practices.

Describe any weaknesses.

Examiner Comments:

Previous Incidents

5. If any bank customers have been a victim of account takeover, confirm that a SAR was filed (You can send an email to the BSA mailbox and request verification). Complete the **Supplemental Assessment.**

Examiner Comments:

Summary of Findings

6. Complete the **Summary of Findings**.

SUMMARY OF FINDINGS

#17 - Account Takeover Risks

Describe all strengths evident from the evaluation.

Describe all weaknesses evident from evaluation, including violations of law/regulation/rules; noncompliance with Departmental policies/guidelines; internal policy deficiencies/ noncompliance; internal control weaknesses; MIS problems; and deficiencies in management supervision.

Report Worthy:

Not Report Worthy:

Determine why weaknesses exist and comment on management's response and plan of action. Identify bank personnel making the response.

SUMMARY RISK RATING ASSIGNED: ☐

Definitions:

1-Strong; 2-Satisfactory; 3-Less than satisfactory; 4-Deficient; 5-Critically deficient; NR-Not Rated

➤ **(Return to Core Analysis)**

Provide copy of this page to EIC/AEIC. Receipt and review of this form by the EIC/AEIC will be evidenced by his/her initials in the appropriate column for this procedure on the SCOPE FORM.

SUPPLEMENTAL ASSESSMENT

If an ATO incident has occurred, perform the following assessment.	
Was a SAR filed? **If not, instruct them to file one per FinCEN Advisory 2011-A016. Issued December 19, 2011**	
When did the incident occur?	
What type of business?	
Was it successful?	
Approximately how much was stolen?	
Approximately how much was recovered?	
Were any of the bank's computers compromised to commit the crime?	
Did the bank make any restitution to the customer?	
If so, How much?	
Did the bank file an insurance claim?	
If so, how much (if anything) was paid by the Insurance company?	
What steps have been taken to prevent recurrence?	

APPENDIX

ATO RESOURCES

Risk Rating Customers

Review the various potential methods listed in the "Best Practices" A bank may choose any method they want. It doesn't have to be a method listed in the "Best Practices." Some banks will simply rate all consumer customers using bill payment services at a lower risk category than corporate customers. This may not be appropriate unless bill payment is restricted to low transaction amounts and a low volume limit. Another option would be to rate all corporate customers with certain online capabilities as high risk. In this case, "individually documented" reviews to determine the risk rating of each customer would not be necessary. However, banks with a moderate or small number of corporate customers may choose to rate their customers individually.

Security Awareness Education for Customers

The extent of educational efforts will vary among banks based on volume of on-line banking customers and customers with different risk ratings. Education efforts will include: user guidelines for the internet banking service and available security features, common security threats, procedures for alerting bank staff of a problem, and developing an incident response plan, etc.

If the bank has not provided security awareness education, suggest optional methods to communicate this information to them (Retail: web page, letters; Corporate: personal visits with customers, group meetings, luncheons. Sample PowerPoint presentation is available on the ECTF website that they can modify and put their name on. Other educational resources are available for customers in Appendix A of the Best Practices).

Person to Person Payments (P2P)

"Person-to-Person" (P2P) payments allow banking customers to send money to family and friends via email or text message.

FDIC Consumer News – Summer 2011 article: Person-to-Person Payments by Smartphone and Mobile Computer Add Convenience and Pose Risks

FFIEC Retail Payments System Handbook – Online Person-to-person (P2P), Account-to-Account (A2A) Payments and Electronic Cash

CATO Best Practices

BestPractices-CATO.pdf

Sample Risk Assessment

sample risk assessment-cato.xls

Project Status Report

CATO Project Status Report.xls

FFIEC Supplemental Guidance on Authentication in an Internet Environment

FFIEC Supplemental Guidance.pdf

FinCEN Advisory regarding SARs for Account Takeover

FIN-2011-A016.pdf